

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002963

International filing date: 17 February 2005 (17.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-057629
Filing date: 02 March 2004 (02.03.2004)

Date of receipt at the International Bureau: 07 April 2005 (07.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

17.02.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 3 月 2 日

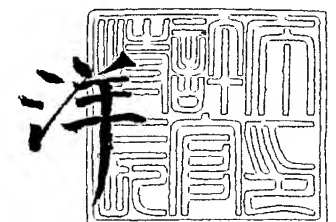
出 願 番 号
Application Number: 特 願 2 0 0 4 - 0 5 7 6 2 9
[ST. 10/C]: [J P 2 0 0 4 - 0 5 7 6 2 9]

出 願 人
Applicant(s): 露 崎 典 平

2 0 0 5 年 3 月 2 5 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 Q00953X0
【あて先】 特許庁長官殿
【国際特許分類】 E05B 49/00
【発明者】
 【住所又は居所】 千葉県茂原市早野 1 8 2 0
 【氏名】 露崎 典平
【特許出願人】
 【識別番号】 595122268
 【氏名又は名称】 露崎 典平
【代理人】
 【識別番号】 100064447
 【弁理士】
 【氏名又は名称】 岡部 正夫
【選任した代理人】
 【識別番号】 100085176
 【弁理士】
 【氏名又は名称】 加藤 伸晃
【選任した代理人】
 【識別番号】 100106703
 【弁理士】
 【氏名又は名称】 産形 和央
【選任した代理人】
 【識別番号】 100096943
 【弁理士】
 【氏名又は名称】 臼井 伸一
【選任した代理人】
 【識別番号】 100091889
 【弁理士】
 【氏名又は名称】 藤野 育男
【選任した代理人】
 【識別番号】 100101498
 【弁理士】
 【氏名又は名称】 越智 隆夫
【選任した代理人】
 【識別番号】 100096688
 【弁理士】
 【氏名又は名称】 本宮 照久
【選任した代理人】
 【識別番号】 100102808
 【弁理士】
 【氏名又は名称】 高梨 憲通
【選任した代理人】
 【識別番号】 100104352
 【弁理士】
 【氏名又は名称】 朝日 伸光
【選任した代理人】
 【識別番号】 100107401
 【弁理士】
 【氏名又は名称】 高橋 誠一郎

【選任した代理人】
【識別番号】 100106183
【弁理士】
【氏名又は名称】 吉澤 弘司
【選任した代理人】
【識別番号】 100120064
【弁理士】
【氏名又は名称】 松井 孝夫
【手数料の表示】
【予納台帳番号】 013284
【納付金額】 21,000円
【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

本体と相手側とのペアによって構成される認証装置であって、該本体、或は相手側、或は本体と相手側の双方に、自発的にランダムパルスを発生するランダムパルス発生器（以下RPGと呼ぶ）と、このRPGが生成するランダムパルスに基づき認証信号を出力する手段と、認証信号を記憶する手段と、認証信号を送信／受信する通信手段と、認証信号の通信制御及び照合等を行う制御手段から成る認証装置。

【請求項 2】

前記制御手段は、ペアを構成する相手側に設けた記憶手段に記憶された認証信号を受信し、受信した認証データを本体に設けた記憶手段の認証データと照合し、その照合結果に従って相手側の認証を行う、また認証の終了後、認証データを更新し、更新された新たな認証データを本体及び相手側の記憶手段に書き込むことを特徴とする請求項 1 に記載の認証装置。

【請求項 3】

更に、制御手段の照合結果に従い駆動装置を制御する駆動装置制御手段を有する、請求項 1 または 2 に記載の認証装置。

【請求項 4】

前記本体は、電子錠の本体であり、前記相手側は、ICカードを含む鍵であることを特徴とする、請求項 1 または 2 に記載の認証装置。

【請求項 5】

前記RPGは、原子核の崩壊で放出される α 粒子、ベータ線またはガンマ線を検出してランダムパルスを発生することを特徴とする請求項 1 乃至 4 のいずれかに記載の認証装置。

【請求項 6】

α 粒子放出体に ^{241}Am 、 ^{210}Pb - ^{210}Po 、 ^{210}Po 、 ^{244}Cm 等を、ベータ線放出体に ^{210}Pb 等を使用することを特徴とする請求項 5 に記載の認証装置。

【請求項 7】

前記RPGは、熱電子、ノイズあるいはジッター等を検出してランダムパルスを発生させることを特徴とする請求項 1 乃至 4 のいずれかに記載の認証装置。

【請求項 8】

前記通信手段は、認証データの送受を赤外線通信あるいは無線通信で行うことを特徴とする請求項 1 乃至 7 のいずれかに記載の認証装置。

【請求項 9】

前記通信手段は、接触による回路接続により、認証データの送受信を行うことを特徴とする請求項 1 乃至 7 のいずれかに記載の認証装置。

【請求項 10】

本体、或は相手側、或は本体と相手側の双方に設けたランダムパルス発生器（以下RPGと呼ぶ）によって自発的にランダムパルスを発生するステップと、このRPGが生成するランダムパルスに基づき認証信号を出力するステップと、認証信号を記憶するステップと、認証信号を送信／受信するステップと、認証信号の通信制御及び照合等を行う制御ステップから成る認証方法。

【請求項 11】

前記制御ステップは、ペアを構成する相手側に設けた記憶手段に記憶された認証信号を受信し、受信した認証データを本体に設けた記憶手段の認証データと照合し、その照合結果に従って相手側の認証を行う、また認証の終了後、認証データを更新し、更新された新たな認証データを本体及び相手側の記憶手段に書き込むことを特徴とする請求項 10 に記載の認証方法。

【請求項 12】

更に、制御手段の照合結果に従い駆動装置を制御する駆動装置制御ステップを有する、請求項 10 または 11 に記載の認証方法。

【請求項 13】

前記RPGは、原子核の崩壊で放出される α 粒子、ベータ線またはガンマ線を検出してランダムパルスが発生することを特徴とする請求項10乃至12のいずれか記載の認証方法。

【請求項14】

α 粒子放出体に ^{241}Am 、 ^{210}Pb - ^{210}Po 、 ^{210}Po 、 ^{244}Cm 等を、ベータ線放出体に ^{210}Pb 等を使用することを特徴とする請求項13に記載の認証方法。

【請求項15】

前記RPGは、熱電子、ノイズあるいはジッター等を検出してランダムパルスが発生させることを特徴とする請求項10乃至12のいずれかに記載の認証方法。

【請求項16】

前記通信ステップは、認証データの送受を赤外線通信あるいは無線通信で行うことを特徴とする請求項10乃至15のいずれかに記載の認証方法。

【請求項17】

前記通信ステップは、接触による回路接続により、認証データの送受信を行うことを特徴とする請求項1乃至15のいずれかに記載の認証方法。

【書類名】明細書

【発明の名称】ランダムパルス発生器 (RPG) を使用した認証装置及び認証方法

【技術分野】

【0001】

本発明は完全なランダムパルスを自発的に発生するランダムパルス発生器を使用して、完全ランダムな信号を認証信号として使用する認証装置及び認証方法に関するものである。

【背景技術】

【0002】

従来の認証装置、例えば電子錠は、鍵メーカーが認証用データをあらかじめ決め、鍵本体（錠）と本体に差し込む鍵とを組として完成させ販売し、使用者は完成品を購入して玄関ドアなど必要な個所に取り付けて使用していた。また電子錠の他のタイプとしては、鍵をかけた時刻を認証データとして鍵本体と鍵とに記憶させ、開錠の際に記憶した認証データを照合するもの（特開平7-233663）、認証データとして声紋を利用したもの（例えば特開平8-257216）等があった。

【特許文献1】特開平7-233663号公報

【特許文献2】特開平8-257216号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

従来の認証装置を、その具体的な適用例である電子錠について考察する。従来の電子錠のうち、メーカーが認証用データを予め決めて製造されたものは、認証用のデータが固定されて自由に変更することが出来ないか（実際は、メーカーがプログラムで認証用データを作成しており、その組み合わせ数に制限があり、同一の認証データが使用される危険があった）、又は、変更が可能なタイプでもテンキーなどの入力であり、使用する桁数や組み合わせが制限されていた。

【0004】

また、多くの場合、メーカーは製造した認証用のデータを保守・サービスのために保存する必要があり、その際に、機密の保持のために膨大な費用をかけていた。例えば、メーカーは、鍵の組み合わせに制限があると、同一認証データが使用される危険が増大するため、同じ組の鍵が同一地域に配布されないよう管理する必要があった。更に、データの漏洩防止は管理者の資質に依存しなければならず、完全な防止対策におのずと限界があった。

なお、同じ認証用のデータが使用されると、電子錠を使用した車などでは同じ駐車場に駐車していた別の車のドアが反応して開く等の不都合が生じる。

【0005】

認証用データとして施錠時の時刻を利用するものであっても、時刻は経時的に順次変化するデータであるから、不規則性を要件とする認証データとしては不適當である。例えば、データの桁数によっては容易に解読されてしまうし、また、同時使用により鍵のコピーが容易に作成されてしまうなどの不都合があり、セキュリティの面で問題があった。

また声紋を利用するタイプのものは、声紋の判定のための装置が複雑となり一般向けの電子錠としては不向きであった。

【0006】

なお、時刻にしても、声紋にしても、いずれも、外部環境に依存するもの（即ち、鍵または鍵本体内で、いかなる環境にも左右されない認証信号を生成することは不可能）であるから、例えばその仕組みを知った人間による人為的な操作より開錠することは可能であって、セキュリティの面で限界があった。

【課題を解決するための手段】

【0007】

本願発明は、上述した従来の認証装置、特に電子錠における問題点を解消するために創

作されたもので、本体と相手側とのペアによって構成される認証装置であって、該本体、或は相手側、或は本体と相手側の双方に、自発的にランダムパルスを発生するランダムパルス発生器（以下RPGと呼ぶ）と、このRPGが生成するランダムパルスに基づき認証信号を出力する手段と、認証信号を記憶する手段と、認証信号を送信／受信する通信手段と、認証信号の通信制御及び照合等を行う制御手段から成る認証装置を提供する。

【0008】

また、本願発明は、該本体、或は相手側、或は本体と相手側の双方に設けたランダムパルス発生器（以下RPGと呼ぶ）によって自発的にランダムパルスを発生するステップと、このRPGが生成するランダムパルスに基づき認証信号を出力するステップと、認証信号を記憶するステップと、認証信号を送信／受信するステップと、認証信号の通信制御及び照合等を行う制御ステップから成る認証方法を提供する。

【発明の効果】

【0009】

本発明に係る認証装置及び認証方法は、例えば、自然崩壊で無限に放出される α 粒子を利用したRPGを鍵本体内部に組み込み、RPGから、環境条件に全く作用されずかつ人的コントロールが一切出来ないオリジナルでランダムな信号を得て、この信号を鍵の認証信号として使用するので、鍵自身においていつでも認証信号の生成が可能で、使用のたびに新しい完全にランダムなデータを書込むことができ、コピー不能とし、そのため、鍵メーカーでのデータ管理が不要で、使用者側で完全なセキュリティを確保でき、安全性が確立出来る等の優れた効果がある。

【発明を実施するための最良の形態】

【0010】

以下、図面を参照し、本発明のランダムパルス発生器（RPG）を使用した認証装置／方法を、電子錠を実施例として詳細に説明する。

図1Aは、本願発明にかかる電子錠の概要を説明する図であり、図1Bは図1Aの電子錠の使用状態を説明する図である。図において、1はドアノブ、2は指紋認証装置、3はテンキー、10は電子錠本体、11は電子錠本体に組み込まれたランダムパルス発生器（以下RPGという）、12は同じく電子錠本体に組み込まれたメモリ、20は鍵、21は鍵に組み込まれたメモリを示す。

【0011】

完全なランダムパルスを発生させるRPGは、本発明者が既に特許権者となっている特許第2926539号に記載されている α 粒子検出装置を使用する。 α 粒子放出体は自然崩壊する ^{241}Am 、 ^{244}Cm 、 ^{210}Pb - ^{210}Po 、 ^{210}Po 等を使用する。金庫のように遮蔽設置スペースがある部位に使用する電子錠であればベータ線やガンマ線を使用しランダムパルスを発生するRPGでも良い。

α 粒子やベータ線、ガンマ線は、温度、圧力、湿度や電磁波など環境に影響されない為、人的制御が出来ない。この特質は他の方法では実現出来ない安全が確保できる重要な要素である。完全な安全性が要求されない部位に使用する電子錠であれば熱電子や半導体のジッターなどをランダムパルスの発生源とするRPGでも良い。

【0012】

鍵本体には、RPGとRPGから送出されるランダムパルスを認証信号として使用できるようにするための電子回路、認証信号を記憶するための回路（記憶素子）、通信の形態に応じた認証信号を送受するための回路、必要に応じ、アンテナ及び通信素子及び電源などが組み込まれる。なお、電源は外部から通信（電磁誘導、電波や端子接続）で供給する方法もある。

まず自発的にランダムパルスを発生するランダムパルス発生器（RPG）11について説明する。

【0013】

RPGは、図2に示すようにパルス発生部11A、プリアンプ部11B、メインアンプ部11C、波形成型部11Dから構成されている。

パルス発生部 11A は鍵(電子錠)が要求される安全度に応じて素子を選択する。最も安全性が要求される鍵については、図 3 に示すような α 粒子放射体に取り付けられた素子(α 放射体付きダイオード)を使用する。図示において、11b はキャンシールを示す。 α 放射体から放出される α 粒子(He 原子)の放出は温度、圧力、電磁波など環境に全く影響されず、電源も不要で自発的に半減期に応じて半永久的に放出される。つまりこの方式では認証に使用する原信号は人的制御が全く出来ない信号源を使用することが出来る事が特徴である。よって外部からは一切変更が出来ない信号発生源となる。なお、放射性カプセルの使用は、前述の特許第 2926539 号に開示がある。

【0014】

鍵取り付け部位が完全な安全性を要求されない場合はパルス発生部を図 4 のようなダイオード(ツェナーダイオード)としても良い。

【0015】

プリアンプ部 11B は、パルス発生部 11A で生成された微小パルス信号をメインアンプ部 11C の入力信号にするための増幅を行う。

メインアンプ部 11C はノイズと明確に区別する為の増幅を行う。この回路でノイズ部が含まれる 0.5V 以下をノイズ信号が含まれる帯域としてディスクリートとする。デスクリートする電圧は要求される信号強度及びノイズレベルに応じて設定すればよい。(図 5 参照)

波形整形部 11D は、メインアンプ部 11C から先頭波形で出力されるパルスを、認証信号として取扱得るようパルス幅を加える。RPG から出力されるパルス波形を図 5 に示す。

【0016】

なお、RPG からの信号を数値化して記憶する方法としては、図 9 に示したように、RPG のランダムパルスは、波高値とパルス間隔がランダムであるので、波高値の電圧をデジタル変換して乱数値とすることもできる。パルスの間隔がランダムであるのでパルス間隔を計測するクロックパルス数を乱数値とする事も出来る。また同図に示すように(電圧、クロックパルス数)の組み合わせとして用いることも出来る。例えば、パルス 1 は (9, 5)、パルス 2 は (4, 3)、パルス 3 は (7, 6)、パルス 4 は (10, 3) 等である。

【0017】

鍵本体の回路を図 6 に示す。鍵本体 10 は、電源モジュール 13、差込検知モジュール 14、トランシーバーモジュール 15、RPG モジュール 16 から構成されている。

電源モジュール 13 は、構成回路全体に動作電源を供給し、図示実施例では、5V の安定化された電圧を供給する DC-DC コンバータ U1 が使用されている。

差し込み検知モジュール 14 は、相手側となる鍵が差し込まれたのを、例えば鍵本体と鍵との接触により検知し(スイッチ SW2 の ON)、バッファ・ゲート U7 を介し、RPG モジュールに起動信号を送る。

【0018】

トランシーバーモジュール 15 は、差し込まれた鍵との間で赤外通通信により信号を送受するモジュールである。U2 は赤外線通信モジュールで、図示実施例で使用されているものは、赤外線発光 LED、フォトダイオード、波形整形 LSI をパッケージ化してある。U3A は単安定マルチバイブレータで、赤外線通信モジュールの出力パルス信号をトリガ入力し、その出力パルス信号を、RPG モジュール U6 に送る。なお、U4 は AND 回路、U5 はインバータ回路で、赤外線通信モジュールの送受信信号の干渉を防いでいる。なお、トランシーバーモジュールは、赤外線通信以外の、光、電波等による無線通信を利用したものであってもかまわない。

図示実施例では、認証データの送受信を、トランシーバーモジュールを使用したものが例示されているが、本願発明はこれに限定されず、通信手段(認証信号の送受手段)は、接触による回路接続であってもよい。

【0019】

RPG モジュール 16 は通信の手順、信号の送出、信号の受信、及びデータの保管をする

とともに、信号発生源であるRPGを組み込んである。RPGモジュールは、また、鍵本体と鍵との認証データが同一であると判別されたときに、電子錠を開錠するための開錠出力を出力する。電子錠の開錠には、公知の手段が使用され、例えば、電磁式のロック機構を持つものであれば、これを制御する手段に制御信号を送り解除を指令する。鍵本体と鍵との通信手順については後述する。

【0020】

図10にRPGモジュールの構成例を示す。このモジュールは、ランダムパルス発生器16A、A/D変換回路16B、基準電圧発生回路16C、クロックパルス発生回路16D、パルスカウンタ16E、入出力端子(入出力回路)16F、演算回路(演算・処理・制御回路)16G、記憶回路16H、表示・動作音出力回路16I、鍵動作出力回路16Jから構成される。演算回路16Gは、入出力端子16Fから入力される認証信号を、記憶回路16Hに記憶した認証信号と一致するか判定する。判定結果は、表示・動作音出力回路16Iに表示され、また、必要に応じ、外部に設けたスピーカから音声で知らせる。一致したときは、鍵動作出力回路を介して開錠出力を出力する。

【0021】

ランダムパルス発生器16Aから出力されるパルスの間隔はランダムであるので、クロックパルス発生回路16Dとパルスカウンタ16Eを用いて、パルス間隔を計測し、そこで得たクロックパルス数を認証信号(認証データ)として利用する。あるいは、ランダムパルス発生器16Aから出力されるパルスの波高値とパルス間隔はランダムであるので、A/D変換回路16Bと基準電圧発生回路16Cを用いて、波高値の電圧をデジタル変換して認証信号(認証データ)として利用することもできる。図示実施例では、いずれの方法でも、あるいは両方を用いて認証信号を得ることができるよう構成してあるが、いずれか一方のみの構成であってもかまわない。

なお、鍵の登録の際には、前述の手段で得た認証データを、記憶回路16Hに記憶し、同時に、入出力端子16Fから、鍵本体側のトランシーバモジュール15に送る。トランシーバモジュールは、認証データを鍵側に送り、鍵側のトランシーバモジュール23を介して動作・記憶モジュール24に記憶される。

【0022】

RPGモジュール16の構成は、図示のものに限定されず、鍵が取り付けられるセキュリティレベルに応じて、内部クロックや判定回路などを構成できるPICやCPUを持つ素子で置き換えることも出来る。ASICにしてワンチップ化することも可能である。

【0023】

鍵本体に挿入する鍵には、認証信号を記憶するための回路と記憶素子、通信の形態に応じた認証信号を送受するための回路、必要に応じ、アンテナ及び通信素子及び電源などが組み込まれる。なお、電源は外部から通信(電磁誘導、電波や端子接続)で供給する方法もある。

【0024】

鍵本体とペアとなる鍵の回路構成を図7に示す。鍵の構成は、電源モジュール22、トランシーバモジュール23、動作・記憶モジュール24から構成される。なお、鍵は、例えばICカードのような形状、構造であってもかまわない。

電源モジュール22は、構成回路全体に動作電源を供給し、図示実施例では、5Vの安定化された電圧を供給するDC-DCコンバータU1が使用されている。本実施例における電源モジュール22は電池の挿入とともに信号電源が供給される構造となっているが、スイッチを押した時に信号の通信が開始するようにスイッチを組み込むことも可能である。

トランシーバモジュール23は、鍵本体との間で赤外通通信により信号を送受するモジュールである。その構成は、鍵本体のトランシーバモジュール15と同様である。ただし、ワンショット・マルチバイブレータU3Aの出力は、動作・記憶モジュール24の非同期受信ポートに送られる。

動作・記憶モジュール24は汎用のPIC(周辺機器接続制御用IC)であって、演算

機能部、メモリ、入出力部等を有し、認証用データを記憶し、鍵本体と鍵との通信、認証データの照合等を制御するプログラムを内蔵する。図示実施例のものは、他に、タイマー、汎用通信ポート等も備えている。

【0025】

次に、鍵本体と鍵との認証手順は、まず認証の相手側としての鍵の登録を行う。鍵の登録は、鍵に差し込めば自動的に認証し、相手側としての登録も可能であるが、取り付けられている装置や部位の安全性のレベルに応じて、図1Aに示すような指紋認証装置2やテンキー3（暗証番号の入力）などと組み合わせる事もできる。

鍵の登録は、鍵を電子錠本体に差し込み、この鍵にRPGからの信号を書き込み、同時に鍵本体に記憶する。

【0026】

使用時の認証は、鍵本体に登録された鍵が差し込まれた時、差込側の鍵から送られてくる認証データが、本体に保存しておいた認証データと一致するか比較する。一致したら開錠する。開錠したらそのデータを削除し、同時に新しい認証データを双方に書き込む。この認証手順と認証データ保存は鍵を使用するたびに行われる。

【0027】

鍵本体と相手側である鍵との間での通信手順の詳細を図8に示す。

- (i) 鍵本体側は、差込検知トリガーマジュールが鍵の挿入を検知するとI(inquire)↓の文字キー（Iコマンド）を相手側である鍵側に送り、照合データの送信を要求する。
- (ii) 鍵側は、鍵本体側からIコマンドを受信すると、保存していた照合データを”R○○○○↓”の文字列（コマンド）で鍵本体側に送信する（○○○○は、RPGのデータにより変化する）。
- (iii) 鍵本体側は、鍵側から照合データを受信すると、本体側で持っていたデータと比較し、不一致であるならばNG音を鳴らして認証を終了する。
- (iv) (iii)において、もし一致しているならば、RPGモジュールから開錠出力を適宜の駆動制御回路に送り、電子錠を開錠する。このとき、同時にRPGモジュールは認証データ（100μsec程度のインターバルデータ）を更新し、新しい認証データとして鍵側に”W○○○○↓”コマンドで送信する。
- (v) Wコマンドを受信すると、鍵側は、その新しいデータを次回の照合のために保存する。
- (vi) 鍵本体側は、Wコマンドで送った認証データが正しく鍵側に受け取られたかどうかを確認するために、再度Iコマンドを鍵側に送信する。
- (vii) 鍵側は、Iコマンドに応答して新しい認証データをRコマンドに付随して鍵本体側に返信する。
- (viii) 鍵本体側は、受信した認証データを照合し、一致しているならば成功と判断しOK音を鳴らす。
- (ix) (viii)において、もし不一致ならば、再度データをWコマンドで鍵側に送信する。以降(v)乃至(viii)までを何回か繰り返し、それでも失敗した場合はFatal Error音を鳴らして認証を終える。

【0028】

Fatal Errorとなった場合は、鍵本体及び鍵双方の保持している認証データが異なったままであるため、このままでは永久に使用できなくなる。これを回避するためには、本願発明では、以下の手順で初期化を実行し強制的に双方が同じデータを保持することができるようになっている。

- (i) RPGモジュールの20ピンをGNDに短絡させる。
- (ii) 鍵をレバースイッチ（差し込み検知トリガーマジュール）に入れる。
- (iii) OK音が鳴れば初期化成功

上記手順は、この方法は、例示であって、これら以外でも初期化は可能であり、安全性が確保できるような方法の選択が重要である。

【0029】

以上、本願発明を、R P G を電子錠本体に組み込んだ例を示し説明したが、本願発明はこれに限定されず IC タグなどに応用できる。R P G は、本体、相手側のいずれか、あるいは双方に組み込むことが可能である。また、本体と相手側との通信手順及び認証手順についても、R P G、メモリ及び通信・認証の制御装置の配置によって変更可能であることは言うまでもない。

【図面の簡単な説明】

【 0 0 3 0 】

【図 1 A】本発明の一実施例に係るランダムパルス発生器（R P G）を使用した鍵の認証装置を示す説明図である。

【図 1 B】図 1 A に示す認証装置の使用状態の説明図である。

【図 2】本発明にかかる実施例に使用されるランダムパルス発生器ブロック図である。

【図 3】本発明に係るランダムパルス発生器に使用する α 放射体付ダイオードを示す正面図である。

【図 4】本発明に係るランダムパルス発生器に使用するツェナーダイオードを示す斜視図である。

【図 5】本発明に係るランダムパルス発生器の出力波形を示すグラフである。

【図 6】本発明に係る鍵本体の側の回路図例を示すブロック図である。

【図 7】本発明に係る鍵側の回路例を示すブロック図である。

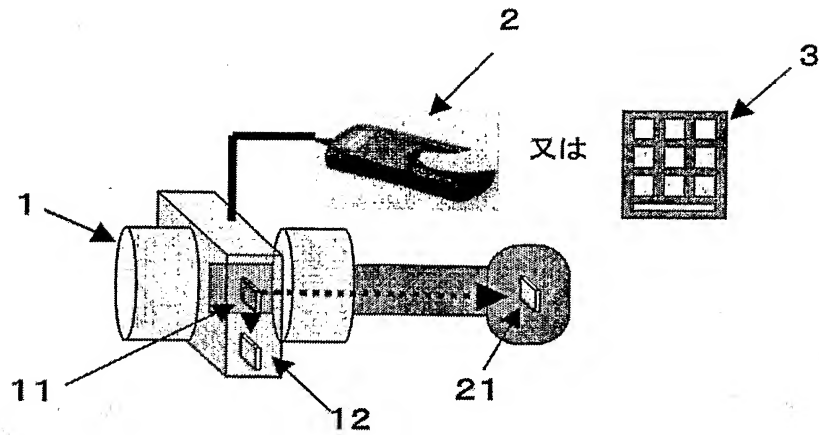
【図 8】本発明に係る鍵本体とペアとなる鍵間の通信手順を示すフローチャートである。

【図 9】本発明に係るランダムパルス発生器の出力パルスの分類表示の方法を示す説明図である。

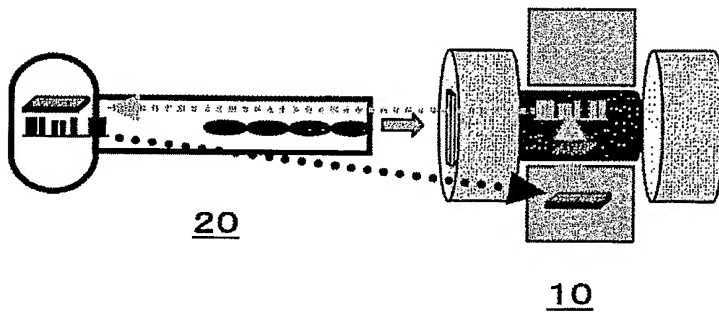
【図 1 0】本発明に係る RPG モジュールの構成例を示すブロック図である。

【書類名】 図面

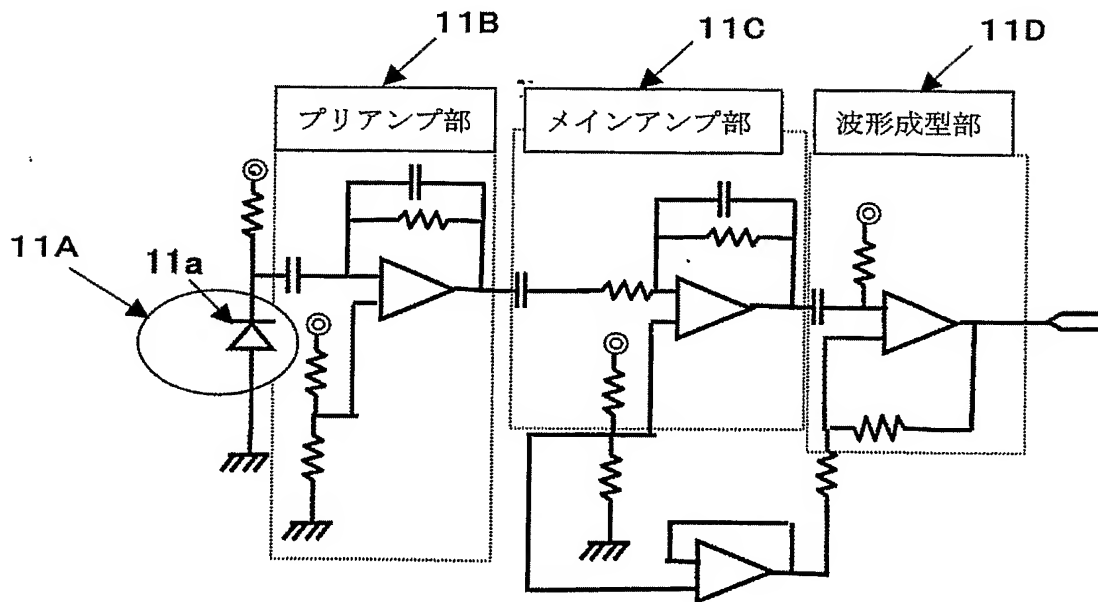
【図 1 A】



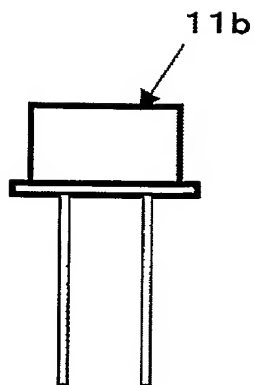
【図 1 B】



【図 2】



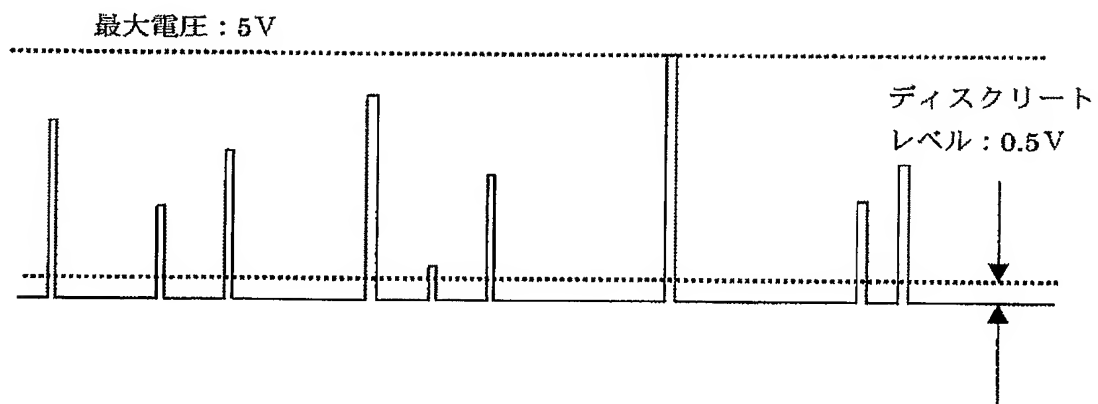
【図 3】



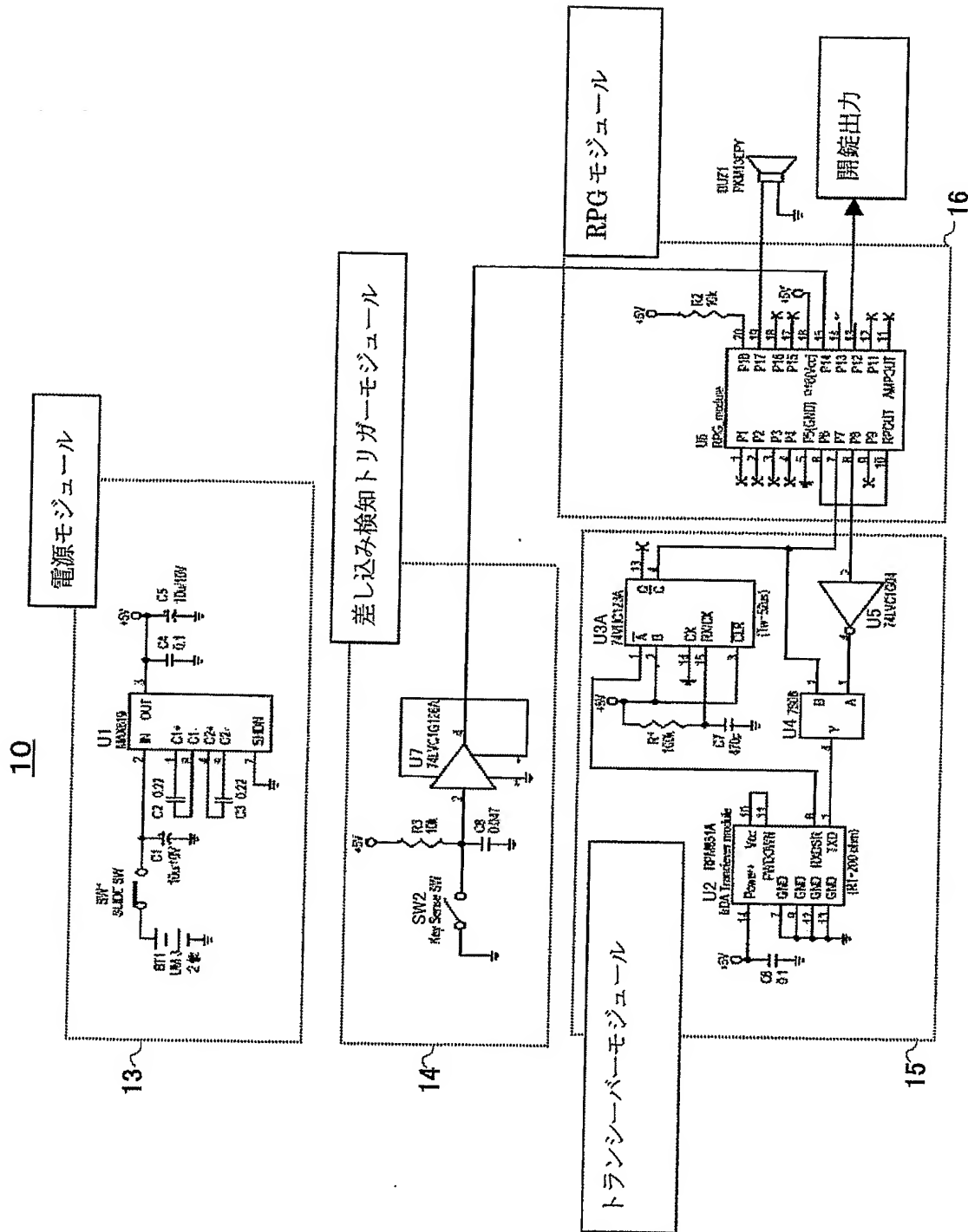
【図 4】



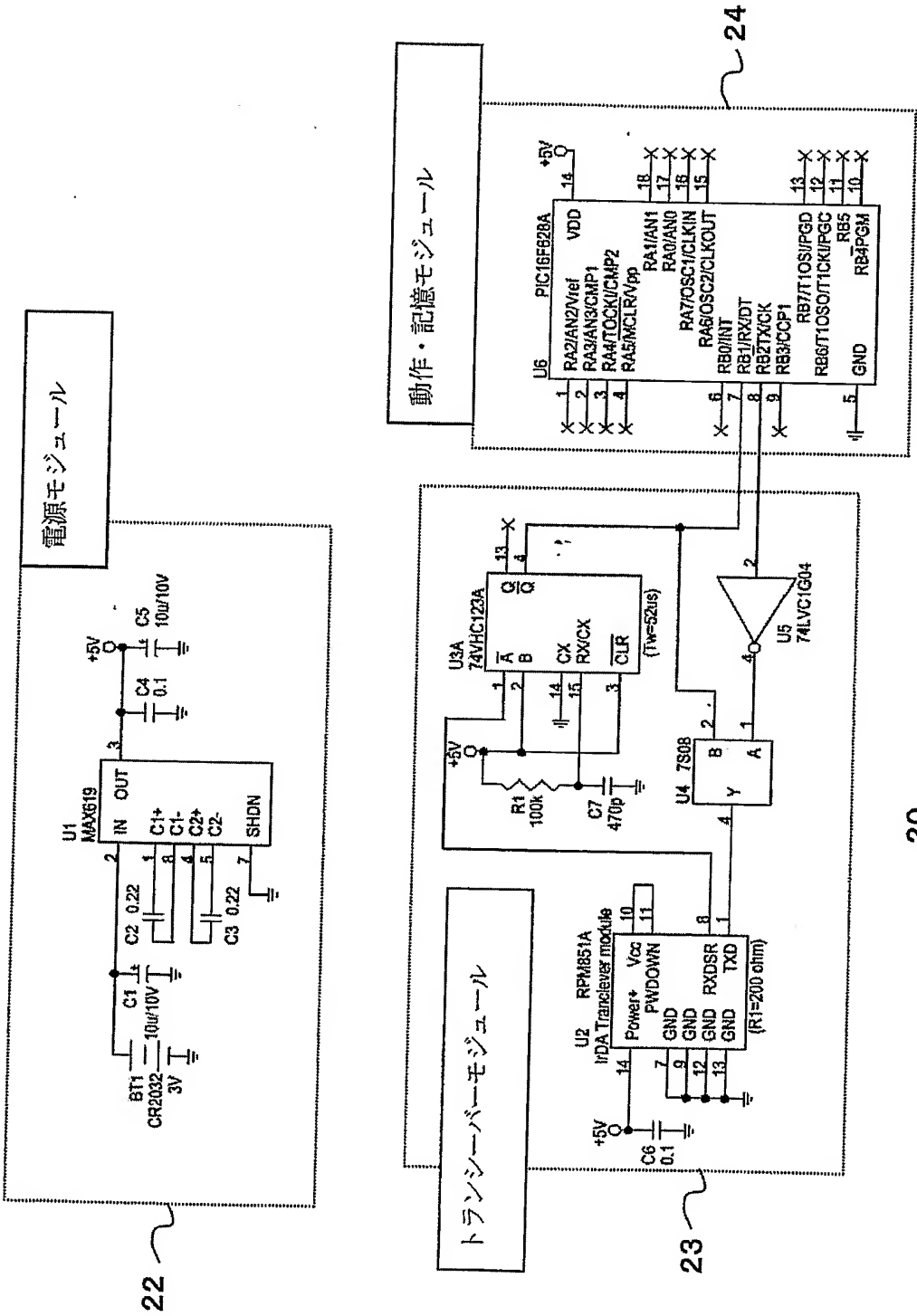
【図 5】



【図 6】

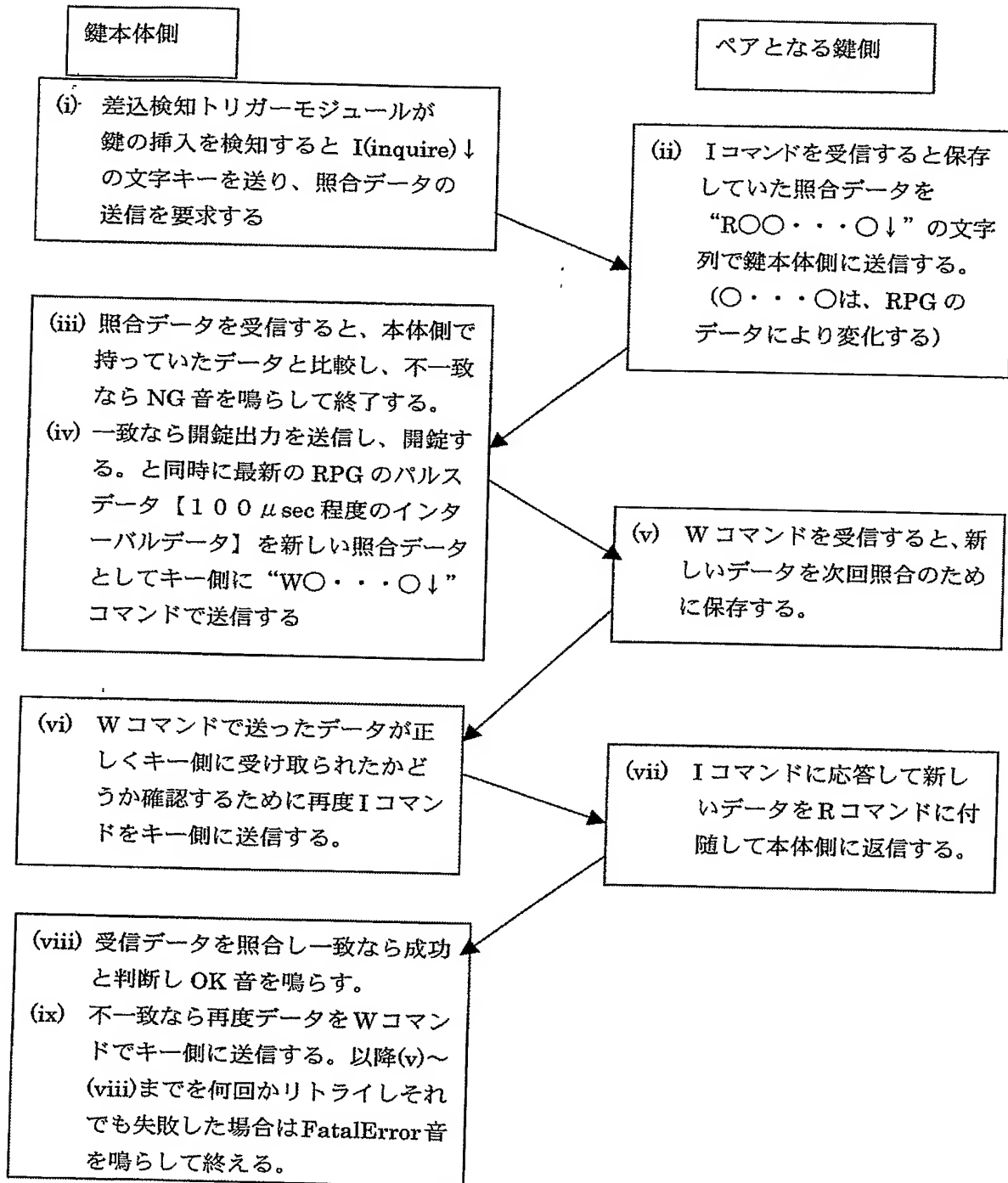


【図 7】

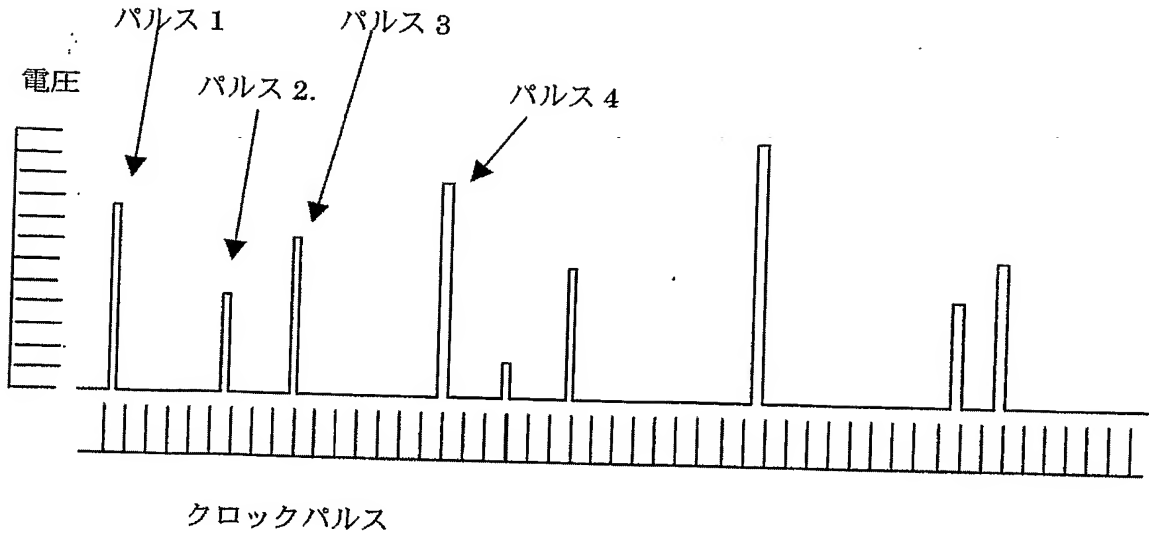


20

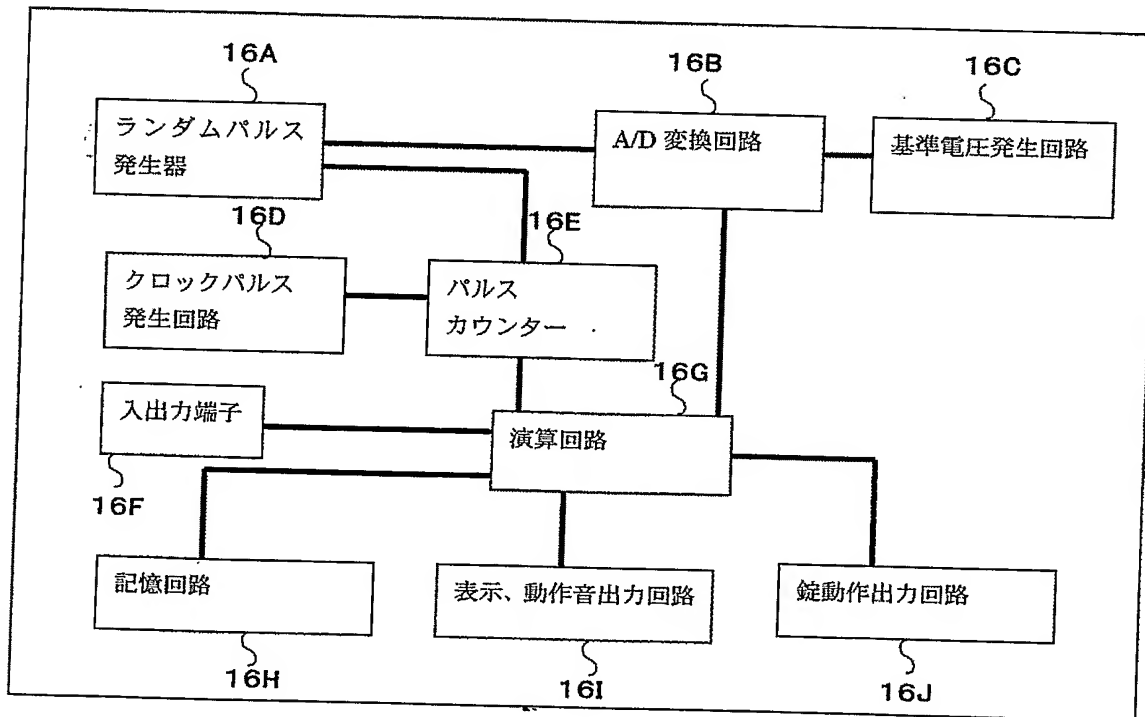
【図 8】



【図 9】



【図 10】



16

【書類名】 要約書

【要約】

【課題】 本発明は完全なランダムパルスを自発的に発生するランダムパルス発生器を使用して、完全ランダムな信号を認証信号として使用する認証装置及び認証方法を提供する。

【解決手段】 本体、或は相手側、或は本体と相手側の双方に、自発的にランダムパルスを発生するランダムパルス発生器（以下RPGと呼ぶ）と、このRPGが生成するランダムパルスに基づき認証信号を出力する手段と、認証信号を記憶する手段と、認証信号を送信／受信する通信手段と、認証信号の通信制御及び照合等を行う制御手段で構成し、使用者側で完全なセキュリティを確保でき、安全性が確立出来る認証装置を提供する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2004-057629
受付番号	50400339930
書類名	特許願
担当官	野本 治男 2427
作成日	平成16年 3月25日

<認定情報・付加情報>

【提出日】 平成16年 3月 2日

特願 2 0 0 4 - 0 5 7 6 2 9

ページ : 1/E

出 願 人 履 歴 情 報

識別番号

[5 9 5 1 2 2 2 6 8]

1. 変更年月日
[変更理由]
住 所
氏 名

1 9 9 5 年 7 月 2 4 日
新規登録
千葉県茂原市早野 1 8 2 0
露崎 典平